

明 細 書

暗号／復号装置及び方法

5 技術分野

この発明は、高いデータ秘守性を保ちデータの同期外れに対する復元性も高い暗号装置、暗号方法および暗号プログラム、復号装置、復号方法および復号プログラム、ならびに、記録媒体に関する。

10 背景技術

従来から、デジタルデータの窃取や改竄などの不正利用を防ぐために、伝送されるデジタルデータに対して暗号化処理を施す暗号化技術が実用化されている。第1図は、デジタルデータの暗号化を行う一例の構成を概略的に示す。暗号化処理を施す前の元データを平文
15 (プレーンテキスト) と称し、平文に暗号化ブロック200で暗号化が施されて暗号文(暗号化データ)が生成される。暗号文は、暗号化ブロック200に対応する復号化ブロック201により暗号を復号化され、元の平文に戻される。

暗号化ブロック200に用いられる暗号化方式としては、例えばA
20 E S (Advanced Encryption Standard) や D E S (Data Encryption Standard) が代表的である。A E S および D E S は、何れも秘密鍵と称される公開されない鍵を用いて平文を暗号化および暗号文の復号化を行う。例えば暗号化ブロック200がA E S により暗号化を行う場合、暗号化ブロック200に入力された平文に対して、秘密鍵である鍵2
25 0 2 を用いて暗号化を施す。暗号化された暗号文は、伝送経路を経由して復号化ブロック201に供給され、暗号化の際に用いられたのと

同じ鍵 2 0 2 を用いて復号化され、元の平文に戻される。これら A E S や D E S は、暗号化と復号化において共通の鍵を用いる共通鍵方式である。

暗号化ブロック 2 0 0 および復号化ブロック 2 0 1 の構成としては
5 、第 2 図に一例が示されるような、暗号化回路や復号化回路として A E S や D E S による暗号器 5 0（または復号器）をそのまま用いる構成が考えられる。この第 2 図の構成は、E C B モード (Electronic CodeBook mode) と称される。第 2 図の構成において、暗号器 5 0 は、入力された平文 M_i を、鍵 (K) を用いて例えば A E S により暗号化して暗号文 C_i を得る。同一の構成において、暗号文 C_i を暗号器 5 0
10 に入力し鍵 (K) を用いて暗号化すると、暗号文 C_i が復号化されて元の平文 M_i が得られる。

この第 2 図の構成では、同一の平文が連続的に入力されると、出力される暗号文も同一の値が続いてしまい、平文と暗号文とに基づく鍵
15 (K) の解読が容易になってしまう。この問題を解決するために、様々な手法が考えられている。

第 3 図 A および第 3 図 B は、暗号器の出力を入力にフィードバックさせる構成であって、C B C モード (Cipher Block Chaining mode) と称する。第 3 図 A に示される暗号化回路 6 0 においては、平文 M_i が
20 E X O R（排他論理和）回路 6 1 を介して暗号器 6 2 に入力され、鍵 (K) を用いて暗号化される。暗号器 6 2 の出力は、暗号文 C_i として出力されると共に、初期値 I V として遅延回路 6 3 により所定の、例えば 1 ワード分の遅延を与えられて E X O R 回路 6 1 に供給され、平文 M_i との排他論理和がとられる。この E X O R 回路 6 1 の出力が
25 暗号器 6 2 に入力される。

第 3 図 B は、対応する復号化回路 6 5 の構成を示す。復号化の際に

は、暗号文 C_i を暗号器 62 に入力すると共に、初期値 IV （イニシャライズベクタ）として遅延回路 67 で所定の、例えば 1 ワード分の遅延を与えて $EXOR$ 68 に供給する。暗号文 C_i は、暗号器 62 で鍵（ K ）を用いて暗号化され、 $EXOR$ 68 により、所定に遅延された初期値 IV との排他論理和をとられて元の平文 M_i に復号化され、出力される。

この第 3 図 A および第 3 図 B に示す構成によれば、初期値 IV を変えることで、同一の鍵（ K ）を用いても、同一の平文 M_i から異なる暗号文 C_i が生成される。初期値 IV として平文 M_i を暗号化した暗号文 C_i を用いているので、同一の平文 M_i が連続的に入力されても暗号器 62 で暗号化された暗号文 C_i は、同一とはならず、上述の ECB モードに比べて暗号文解析が難しくなる。

第 4 図 A および第 4 図 B は、発生した暗号文 C_i の一部を暗号器の入力としてフィードバックさせる構成であって、CFB モード (Cipher FeedBack mode) と称する。第 4 図 A に示される暗号化回路 70 においては、 j ビットデータとして入力された平文 M_i が $EXOR$ 回路 71 に供給され、暗号器 74 の出力のうち j ビットと排他論理和がとられ、暗号文 C_i として出力される。この出力は、ビット数を j ビットから k ビットに変換する回路 72 を介して DR 回路 73 に供給される。DR 回路 73 は、シフトレジスタを有し、入力された k ビットのデータを入力順にシフトさせ、例えば 128 ビットのデータ X_i を発生させる。データ X_i は、暗号器 74 に供給され、鍵（ K ）を用いて暗号化され 128 ビットのデータ Y_i とされる。このデータ Y_i は、擬似的な乱数列であって、入力される平文 M_i とで排他論理和をとることで、暗号文 C_i が生成される。

第 4 図 B は、対応する復号化回路 75 の構成を示す。 j ビットデー

タとして入力された暗号文 C_i は、 \oplus 回路 76 で k ビットデータに変換され DR 回路 78 に供給されると共に、EXOR 回路 77 に供給される。DR 回路 78 は、シフトレジスタを有し、供給された k ビットのデータから例えば 128 ビットのデータ X_i を生成し、暗号器 79
5 に供給する。データ X_i は、暗号器 79 で鍵 (K) を用いて暗号化され 128 ビットのデータ Y_i とされる。このデータ Y_i は、擬似的な乱数列であって、入力された暗号文 C_i との排他論理和をとることで暗号文 C_i が元の平文 M_i に復号化される。

この CFB モードは、入力された平文 M_i や暗号文 C_i をシフトレジスタに入力し、それを暗号器に入力して疑似乱数列を発生させるので、連続的に平文 M_i が入力されるストリームデータの暗号化に適している一方、暗号化回路 75 から出力された暗号化データに例えば伝送系などでエラーが生ずると、シフトレジスタ (DR 回路) が一巡するまでエラーから回復できないという欠点がある。

15 第 5 図 A および第 5 図 B は、暗号器の出力だけをフィードバックして疑似乱数を発生させる構成であって、OFB モード (Output Feedback mode) と称する。第 5 図 A に示される暗号化回路 80 では、暗号器 83 自身の出力をシフトレジスタを有する DR 回路 82 を介して暗号器 83 に入力し、それを鍵 (K) を用いて暗号化する。暗号器 83 から出力されたデータ Y_i は、疑似乱数列であって、このデータ Y_i の
20 うち j ビットだけを EXOR 81 回路に供給し、 j ビットデータとして入力される平文 M_i との排他論理和をとることで、平文 M_i が暗号文 C_i とされ出力される。

第 5 図 B は、対応する復号化回路 85 の構成を示す。この OFB モードでは、復号化回路 85 は暗号化回路 80 と同一の構成とされる。
25 すなわち、 j ビットの暗号文 C_i が EXOR 回路 86 に入力される。

一方、暗号器 8 8 自身の出力がシフトレジスタを有する D R 回路 8 7 を介して暗号器 8 8 に入力され、鍵 (K) を用いて暗号化される。暗号器 8 8 から出力されたデータ Y i は、疑似乱数列であって、このデータ Y i のうち j ビットだけを E X O R 8 6 に供給し、入力された暗号文 C i との排他論理和をとることで、暗号文 C i が平文 M i に復号化される。

この O F B モードは、暗号化回路 8 0 内および復号化回路 8 5 内でフィードバックが完結しているため、伝送系エラーなどの影響を受けないというメリットがある。

10 第 6 図 A および第 6 図 B は、カウンタの出力を順次カウントアップしていき、それを暗号器の入力に与える構成であって、カウンタモード (Counter Mode) と称される。すなわち、カウンタモードでは、カウンタの出力が暗号化されて用いられる。第 6 図 A に示される暗号化回路 9 0 では、1 2 8 ビット出力のカウンタ 9 2 が順次カウントアップされたカウント値 X i が暗号器 9 3 に入力され、鍵 (K) を用いて暗号化される。暗号器 9 3 から出力されるデータ Y i は、疑似乱数列であって、このデータ Y i のうち j ビットだけを E X O R 回路 9 1 に供給し、j ビットで入力された平文 M i との排他論理和をとることで、暗号文 C i が生成される。

20 第 6 図 B は、対応する復号化回路 9 5 の構成を示す。このカウンタモードでは、復号化回路 9 5 は暗号化回路 9 0 と同一の構成とされる。すなわち、カウンタ 9 7 で順次カウントアップされたカウント値 X i が暗号器 9 8 に入力され、鍵 (K) を用いて暗号化される。暗号器 9 8 から出力されるデータ Y i は、疑似乱数列であって、このデータ Y i のうち j ビットだけを E X O R 回路 9 6 に供給し、j ビットで入力された暗号文 C i との排他論理和をとることで、暗号文 C i が平文

M i に復号化される。

上述のように、C F Bモード、O F Bモードおよびカウンタモードでは、暗号文C i は、暗号化を行った同一の疑似乱数と暗号文C i との排他論理和をとることで、復号化される。非特許文献「Douglas R.
5 Stinson、櫻井幸一、「暗号理論の基礎」、共立出版株式会社、1996年」に、上述したような種々の暗号化方式が記載されている。

ところで、近年では、映画館などにおいて、例えば映像サーバに蓄積された映像データを再生し、スクリーンに投影して映画の上映を行うようにした、デジタルシネマシステムが提案されている。このシ
10 ステムによれば、例えばネットワークを介して配信された映像データや、大容量光ディスクなどの記録媒体に記録された映像データが映像サーバに供給される。そして、映像サーバからプロジェクタに対して例えば同軸ケーブルを介してこの映像データが伝送され、プロジェクタによりスクリーンに映像データに基づく映像が投影される。

15 映像データは、例えばH D - S D I (High Definition-Serial Data Interface)による伝送フォーマットにより、シリアルデジタルデータとして映像サーバからプロジェクタに伝送される。この映像データは、ベースバンドのビデオデータとして伝送され、その伝送レートは、例えば略1.5 G b p s (Giga bits per second)とされる。

20 このとき、映像データの窃取を防ぐために、映像サーバから出力される映像データを暗号化し、暗号化された映像データを例えば同軸ケーブルに対して出力してプロジェクタに伝送する。ここで、H D - S D I のフォーマットにおいて伝送されるコードに制約が無ければ、上述した各暗号化方式を用い、H D - S D I の暗号化／復号化システム
25 が実現できることになる。すなわち、映像サーバ側に暗号化回路を設け、出力される映像データに暗号化を施す。また、プロジェクタ側に

映像サーバの暗号化回路に対応する復号化回路を持たせる。映像サーバで暗号化された映像データは、HD-SDIのフォーマットに乗せられて同軸ケーブルを介してプロジェクタに伝送され、プロジェクタの復号化回路で暗号を復号化され、ベースバンドのビデオデータに戻
5 される。

しかしながら、実際には、上述のHD-SDIには、ワード同期用に禁止コードが定義されている。そこで、本願発明の出願人により、この禁止コードを発生させないで暗号化を行う方式が特願2002-135039として既に出願されている。また、当該出願の関連出願
10 として、特願2002-135079、特願2002-135092、特願2002-173523および特願2002-349373が既に出願されている。

さらに、近年では、HD-SDIにおけるビデオデータの暗号化／復号化に関する標準化が進められており、暗号化方式として、第6図
15 Aおよび第6図Bを用いて説明したカウンタモードを用いることが提案されている。この提案によれば、暗号化単位の128ビットのデータを分割して用い、分割されたそれぞれのビットに対して下記の3種類のカウンタを適用するようにしている。

- (1) 暗号器のクロック毎にカウントアップするクロックカウンタ
- 20 (2) 映像データのライン毎にカウントアップするラインカウンタ
- (3) 映像データのフレーム毎にカウントアップするフレームカウンタ

これら3種類のカウンタのうち(1)のクロックカウンタは、ラインが更新される毎にリセットされ、(2)のラインカウンタは、フレームが更新される毎にリセットされ、(3)のフレームカウンタは、
25 映像データによる1つのプログラムの開始時に一度だけリセットされ

る。このように、カウント周期およびリセットタイミングが異なる複数のカウンタを組み合わせることで、例えばデータの伝送系において同期外れ、データ欠落などが生じて、失われるすなわち復号できないデータは、最大で1ライン分のデータで済ませることができる。

また、(1)のクロックカウンタや(2)のラインカウンタによるリセットを行っても、(3)のフレームカウンタの値が更新されていくので、同一の疑似乱数列が繰り返されることが無いという利点もある。

- 10 これに対して、第4図Aおよび第4図Bを用いて説明したCFBモードを用いる場合には、若し、プログラム開始後のある時点でリセットをかけ、その後リセットをかけないとしたら、上述した同期外れや、データの欠落などの事故が発生した場合、復帰が非常に困難である。つまり、このCFBモードにおいては、暗号化回路の出力をシフト
- 15 レジスタにより順次シフトさせていったデータを暗号器で鍵(K)を用いて暗号化し、この暗号器の出力を用いて平文 M_i の暗号化を行っている。そのため、暗号化の際にある時点でエラーが発生すると、シフトレジスタによる影響が無くなるまで復号可能なデータが出力されない。換言すれば、CFBモードにおいては、出力される暗号文 C_i
- 20 は、過去の全ての暗号文 C_i に依存しているため、短時間に復元することができない。

- 勿論、CFBモードでも、フレーム毎、ライン毎に暗号器の入力をリセットすることが可能である。しかしながら、CFBモードでフレーム毎、ライン毎にリセットを行った場合、例えば画面全体が黒一色
- 25 といった均一な入力データが複数フレームにわたって入力された場合には、暗号器から出力される疑似乱数列は、フレーム毎に同一の並び

となってしまう。このようなケースが発生すると、例えば映像サーバとプロジェクタ間で伝送されるデータを窃取して暗号を解読する際の重大なヒントになってしまい、暗号のセキュリティー上、好ましくない。

- 5 ここで、上述のデジタルシネマシステムにおける映像データの窃取方法について考える。第7図は、この映像データ窃取を実現するための一例のシステムを概略的に示す。映像データは、映像サーバ250で再生されて暗号化され、暗号データとして同軸ケーブル251に送り出される。暗号化方式としては、伝送系のエラーに対する復元性を考慮し、上述したカウンタモードにおいて映像データのライン毎、
10 フレーム毎、プログラムの先頭でそれぞれカウンタをリセットする方式を用いる。プロジェクタ254側では、本来であれば、プロジェクタ254に接続された同軸ケーブル251を介して送られてくるデータを受け取り、暗号を復号化してベースバンドの映像データとし、スクリーン255に映出する。
15

- 映像データの窃取者は、データ窃取記録／交換装置252、ビデオカメラ256およびビデオデータ記録装置257を用意する。データ窃取記録／交換装置252は、映像サーバ250およびプロジェクタ254の間に挿入する。例えば、第7図に示されるように、サーバ250とプロジェクタ254とを接続すべき同軸ケーブル251をデータ窃取記録／交換装置252に接続し、データ窃取記録／交換装置252の出力を同軸ケーブル253でプロジェクタ254に送る。ビデオカメラ256は、スクリーン255に投影された映像を撮影可能に配置される。ビデオカメラ256で撮影された映像は、ビデオデータ
20 記録装置257に供給され、光ディスクや磁気テープなどの記録媒体に記録される。
25

- このような構成において、窃取者は、映像サーバ 250 から出力される、映像データが暗号化された暗号化データと、映像データに付随するメタデータとをデータ窃取記録／交換装置 252 で記録する。データ窃取記録／交換装置 252 は、映像サーバ 250 から供給された
- 5 暗号化データの代わりに、予め用意した所定データを、映像サーバ 250 から暗号化データに付随されて供給されたメタデータと共に出力する。このとき、メタデータには手を加えない。なお、データ窃取記録／交換装置 252 で予め用意される所定データは、例えば黒一色の画面を表示するための固定値である。
- 10 データ窃取記録／交換装置 252 から出力された所定データとメタデータは、プロジェクタ 254 に供給される。プロジェクタ 254 では、供給された所定データを復号化する。すなわち、所定データが黒一色を表示する固定データである場合、所定データと復号化回路における疑似乱数とが排他論理和演算される。この所定データと疑似乱数
- 15 とが排他論理和演算されてなる映像データがスクリーン 255 に投影される。
- スクリーン 255 に投影される映像は、このように、例えば固定値である所定データに暗号化回路による疑似乱数を作用させたデータに基づくので、絵としては映像サーバ 250 から出力された元の映像データとは全く異なり、ノイズとしか見えないような映像となる。窃取者は、このスクリーン 255 に投影された上述の所定データによる映像をビデオカメラ 256 で撮影し、ビデオデータ記録装置 257 で記録する。このデータ窃取記録／交換装置 252 で記録された暗号化データと、ビデオデータ記録装置 257 で記録された映像データとに基づき、暗号データ化の元の映像データを復元することができる。
- 20 すなわち、プロジェクタ 254 の映写性能と、ビデオカメラ 256

の撮像性能とが理想的なものであれば、これら暗号化データと映像データの排他論理和をとることで、暗号化データの元の映像データを復元できることになるという問題点があった。

現実的には、理想的な性能を備えたプロジェクタ 2 5 4 やビデオカメラ 2 5 6 は存在しないので、上述の方法でも、正確に元の映像データを復元することはできない。しかしながら、不完全なデータを用いても、上述の演算を行うことで、高い確率で元の映像データの再現を行うことが可能である。

例えば、映像データの性質として、ある画素とその画素に近接した画素とでは、高い相関性があることが知られている。この近接画像の相関性を利用して、上述のような状況下において、正確に再現できなかった画素の値を求めることができる。その結果、その画素（映像データを暗号化した際の疑似乱数を絞り込んでいくことができってしまう。これにより、窃取者により、映像データの暗号化の際の鍵（K）を解読する大きな手がかりを得られてしまうという問題点があった。

一方、映像サーバ 2 5 0 から出力される映像データに対して暗号化を行う暗号化方式として C F B モードを用いれば、この方式では暗号化された暗号化データをフィードバックして入力データの暗号化を行っているため、同一のデータを入力し続けても出力される疑似乱数列が変化する。そのため、上述のような窃取方法では鍵（K）の手がかりを得ることが困難である。しかしながら、上述したように、C F B モードは、伝送系のエラーに対する復元性が弱いという問題点があった。これは、実際に映画館での上映などに用いる際に、深刻な問題となりうる。

25

発明の開示

したがって、この発明の目的は、より秘守性に優れ、尚かつ、伝送系のエラーに対する復元性も高い暗号化を行うことができる暗号装置、暗号方法および暗号プログラム、復号装置、復号方法および復号プログラム、ならびに、記録媒体を提供することにある。

- 5 この発明は、上述した課題を解決するために、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする 1 または複数のカウンタと、保持
- 10 手段で保持されたデータと 1 または複数のカウンタによる 1 または複数のカウント値とを暗号化する暗号化手段と、暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算手段と、演算手段から出力された暗号化データの一部または全部
- 15 を保持手段に入力する経路と、保持手段および 1 または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持手段および 1 または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有することを特徴とする暗号装置である。
- 20 また、この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする 1 または複数のカウンタのステップと、保持のステップ
- 25 プで保持されたデータと 1 または複数のカウンタのステップによる 1 または複数のカウント値とを暗号化する暗号化のステップと、暗号化

- のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生ステップとを有することを特徴とする暗号方法である。
- 10 この発明は、入力されたデータの一部または全部をトリガ信号により保持し、保持されたデータをリセット信号によりリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウンタのステップと、保持のステップで保持されたデータと1または複数のカウンタのステップによる1または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生ステップとを有する暗号方法をコンピュータ装置に実行させることを特徴とする暗号プログラムである。
- 25

この発明は、入力されたデータの一部または全部をトリガ信号によ

り保持し、保持されたデータをリセット信号によりリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウントのステップと、保持のステップで保持されたデータと1または複数のカウントのステップによる1または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生 of theステップとを有する暗号方法をコンピュータ装置に実行させる暗号プログラムが記録されたことを特徴とするコンピュータ装置に読み取り可能な記録媒体である。

また、この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウンタと、保持手段で保持されたデータと1または複数のカウンタによる1または複数のカウント値とを暗号化する暗号化手段と、暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算手段と、演算手段から出力された暗号化データの一部または全部を保持手段に入力する経路

と、保持手段および1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持手段および1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有する暗号装置で暗号化された暗号化データを復号する復号装置において、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウンタと、保持手段で保持されたデータと1または複数のカウンタによる1または複数のカウント値とを暗号化する暗号化手段と、暗号化手段の出力と外部から入力された暗号化データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算手段と、外部から入力された暗号化データの一部または全部を保持手段に入力する経路と、保持手段および1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持手段および1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有することを特徴とする復号装置である。

また、この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウンタのステップと、保持のステップで保持されたデータと1または複数のカウンタのステップによる1または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の

規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生 of the ステップとを有する暗号方法で暗号化された暗号化データを復号する復号方法において、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウンタのステップと、保持のステップで保持されたデータと1または複数のカウンタのステップによる1または複数のカウンタ値とを暗号化する暗号化手段と、暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、外部から入力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生 of the ステップとを有することを特徴とする復号方法である。

この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたは

- カウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウントのステップと、保持のステップで保持されたデータと1または複数のカウントのステップによる1または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生
- 5 のステップとを有する暗号方法で暗号化された暗号化データを復号する復号方法をコンピュータ装置に実行させる復号プログラムにおいて、復号方法は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウントのステップと、保持のステップで保持されたデータと1または複数のカウントのステップによる1または複数のカウント値とを暗号化する暗号化手段と、暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、外部から入力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウ
- 10
- 15
- 20
- 25

ンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生ステップとを有することを特徴とする復号プログラムである。

この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウントのステップと、保持のステップで保持されたデータと1または複数のカウントのステップによる1または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生ステップとを有する暗号方法で暗号化された暗号化データを復号する復号方法をコンピュータ装置に実行させる復号プログラムが記録されたコンピュータ装置に読み取り可能な記録媒体において、復号方法は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウントのステップと、保持のステップで保持されたデータと1または複数のカウントのステップによる1または

- 複数のカウント値とを暗号化する暗号化手段と、暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、外部から入力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有することを特徴とする記録媒体である。
- 10 上述したように、この発明では、最終的な暗号化データの一部または全部がトリガ信号により保持されリセット信号によりリセットされる保持された暗号化データとトリガ信号によりカウント値をカウントアップまたはカウントダウンしリセット信号によりカウント値が所定の値にリセットされる1または複数のカウント値とを暗号化した出力と、外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化して最終的な暗号化データとして出力するようにされ、最終的な暗号化データが暗号化されるデータにフィードバックされると共に、暗号化データを得るための演算に用いる暗号化の出力がリセット信号によりリセットされるため、同一データの連続入力を
- 15 利用したデータ窃取が行えないと共に、暗号化データの伝送系によるデータエラーなどに対する復元力を有する。

- この発明によれば、暗号化回路にC F Bモードを取り入れ、ビデオデータの暗号化の際に、出力された暗号化データを暗号器の入力にフィードバックしているため、従来技術で第7図を用いて説明したようなデータ窃取方法で暗号化画像データを窃取して元の画像データを復元しようとしても、元の画像データを全く復元することができないと
- 25

いう効果がある。これは、C F Bモードの特徴として、暗号器で発生される疑似乱数列が入力データ列に影響されるため、従来技術で説明した窃取方法により得られた疑似乱数列と、暗号化回路において暗号器で発生される疑似乱数列とが全く異なるからである。

- 5 また、この発明によれば、暗号化データを暗号器の入力にフィードバックさせる際に、フィードバックする暗号化データをホールドし、ホールドされた暗号化データをライン毎にリセットしているため、前ラインでの暗号化データによるフィードバックの影響が全くなり、前ラインで同期外れや画素欠落などの事故が生じた場合でも、ラインが更新された際に完全に復帰できるという効果がある。
- 10

図面の簡単な説明

- 第1図は、デジタルデータの暗号化を行う一例の構成を概略的に示すブロック図、第2図は、E C Bモードによる暗号化回路の一例の構成を示すブロック図、第3図Aおよび第3図Bは、C B Cモードによる暗号化回路の一例の構成を示すブロック図、第4図Aおよび第4図Bは、C F Bモードによる暗号化回路の一例の構成を示すブロック図、第5図Aおよび第5図Bは、O F Bモードによる暗号化回路の一例の構成を示すブロック図、第6図Aおよび第6図Bは、カウンタモードによる暗号化回路の一例の構成を示すブロック図、第7図は、映像データ窃取を実現するための一例のシステムを概略的に示すブロック図、第8図は、この発明の実施の一形態に適用可能な映像投影システムの一例の構成を概略的に示すブロック図、第9図は、H D - S D I暗号化装置の一例の構成を示すブロック図、第10図は、この発明の実施の一形態による暗号化回路の一例の構成を示すブロック図、第11図は、この発明の実施の一形態による暗号化回路に対応する復号
- 15
- 20
- 25

化回路の一例の構成を示すブロック図である。

発明を実施するための最良の形態

以下、この発明の実施の一形態を、図面を参照しながら説明する。

- 5 第8図は、この発明の実施の一形態に適用可能な映像投影システムの一例の構成を概略的に示す。この映像投影システムは、デジタルデータとして提供された映像データを映画館などで上映する際に用いて好適なものである。ビデオデコーダ10は、例えば図示されない映像サーバからネットワークなどを介して供給された、圧縮符号化された
- 10 映像データをデコードし、ベースバンドのビデオデータとする。このビデオデータは、例えばHD-SDIのフォーマットに乘せられ、伝送レートが略1.5Gbpsのシリアルデジタルデータとして出力される。

- なお、ビデオデコーダ10は、例えば大容量の光ディスクといった
- 15 記録媒体に圧縮符号化されて記録された映像データをビデオデコーダ10で再生し、デコードして出力するようにしてもよい。

- ビデオデコーダ10から出力されたデータは、同軸ケーブル11を介してHD-SDI暗号化装置12に供給される。HD-SDI暗号化装置12は、供給されたデータから映像データを抽出して暗号化を
- 20 施し、暗号化ビデオデータとし、この暗号化ビデオデータを再びHD-SDIのフォーマットに乘せて出力する。暗号化の際の鍵(K)は、例えば、RS232Cなどのインターフェイスを介して接続されたコンピュータ装置(PC)から供給される。HD-SDI暗号化装置12から出力されたデータは、同軸ケーブル13を介してプロジェク
- 25 タ16側に伝送され、HD-SDI復号化装置14に供給される。

HD-SDI復号化装置14は、HD-SDIフォーマットのディ

デジタルデータから暗号化ビデオデータを抽出して暗号を復号化し、元のベースバンドのビデオデータに戻す。復号化の際の鍵（K）は、HD-S-D-I 暗号化装置 12 において暗号化の際に用いられた鍵（K）と共通の鍵が用いられ、例えば、RS-232C などのインターフェ
5 イスを介して接続されたコンピュータ装置から供給される。

HD-S-D-I 復号化装置 14 で復元されたベースバンドのビデオデータは、同軸ケーブル 15 を介してプロジェクタ 16 に供給され、プロジェクタ 16 により図示されないスクリーンに投影される。

なお、上述では、ビデオデコーダ 10 と HD-S-D-I 暗号化装置 1
10 2 とが別個の装置であるように説明したが、実際には、HD-S-D-I 暗号化装置 12 は、ビデオデコーダ 10 に組み込まれて用いられる。この場合には、ビデオデコーダ 10 と HD-S-D-I 暗号化装置 12 とを接続する同軸ケーブル 11 を省略することができ、また、ビデオデ
15 コーダ 10 から出力されるビデオデータを HD-S-D-I のフォーマットに乗せずに、例えばパラレルのデジタルデータとして扱うことができる。HD-S-D-I 復号装置 14 も同様にして、プロジェクタ 16 に組み込まれて用いられる。この場合にも同様に、同時期ケーブル 15 を省略することができると共に、HD-S-D-I 復号装置 14 からパ
20 ラレルデジタルデータとしてビデオデータを出力することができる。

第 9 図は、HD-S-D-I 暗号化装置 12 の一例の構成を示す。HD-S-D-I 暗号化装置 12 は、概略的には、HD-S-D-I シリアル／パラレル変換回路ブロック 20、暗号回路ブロック 30 および HD-S-D-I パラレル／シリアル変換回路ブロック 40 から構成される。

25 HD-S-D-I フォーマットに乗せられ、同軸ケーブル 11 を介して伝送されたデジタルデータは、HD-S-D-I シリアル／パラレル変

- 換回路ブロック 20 に供給されてパラレルのデジタルデータに変換され、ビデオデータ、オーディオデータおよびメタデータが取り出される。オーディオデータおよびメタデータは、HD-SDI パラレル／シリアル変換回路ブロック 40 に供給され、ビデオデータは、暗号化回路ブロック 30 で暗号化されて HD-SDI パラレル／シリアル変換回路ブロック 40 に供給される。HD-SDI パラレル／シリアル変換回路ブロック 40 では、オーディオデータおよびメタデータと、暗号化された暗号化ビデオデータとを重畳し、HD-SDI フォーマットに準じたシリアルデジタルデータに変換して出力する。
- 10 HD-SDI シリアル／パラレル変換回路ブロック 20 において、入力された HD-SDI フォーマットのシリアルデジタルデータは、ケーブルイコライザ (EQ) ／クロック復元回路 21 で、伝送時に同軸ケーブル 11 により劣化した周波数特性が補正されると共に、クロックが抽出される。デジタルデータは、受信時に信号が反転しても受信可能なように、NRZI 符号化されて信号の方向性が除去されている。
- 15 ケーブルイコライザ／クロック復元回路 21 から出力されたデジタルデータは、NRZI 回路 22 に供給され、送信時に施された NRZI 符号が復号化される。NRZI 回路 22 の出力は、デスクランブラ 23 でデータの送信時に DC 成分を除去するために施されたスクランブル処理が解除され、シンク検出回路 24 でワード同期が検出され、検出されたワード同期に基づきシリアル／パラレル変換回路 25 でパラレルのデジタルデータに変換される。
- シリアル／パラレル変換回路 25 の出力は、デマルチプレクサ 26 に供給され、多重化されているビデオデータ、オーディオデータおよびメタデータなどが分離される。デマルチプレクサ 26 で分離されたオーディオデータおよびメタデータは、HD-SDI パラレル／シ
- 25

アル変換回路ブロック 40 のマルチプレクサ／フォーマッタ 41 に供給される。

一方、デマルチプレクサ 26 で分離されたビデオデータは、暗号回路ブロック 30 に供給され、暗号化回路 31 で暗号化される。暗号回路ブロック 30 は、CPU (Central Processing Unit) 32 を有し、例えば RS-232C といった所定のインターフェイスを介して外部のコンピュータ装置と通信を行うことができる。暗号回路ブロック 30 そのものをコンピュータ装置で構成し、例えば所定の記録媒体に記録されて提供される暗号化プログラムに従い、暗号化処理を行わせてもよい。暗号化回路 31 において暗号化の際に用いられる鍵 (K) は、外部のコンピュータ装置から所定のインターフェイスを介して供給され、CPU 32 を介して暗号化回路 31 に与えられる。暗号化回路 31 で暗号化された暗号化ビデオデータは、HD-SDI パラレル／シリアル変換回路ブロック 40 のマルチプレクサ／フォーマッタ 41 に供給される。

HD-SDI パラレル／シリアル変換回路ブロック 40 において、マルチプレクサ／フォーマッタ 41 は、供給されたオーディオデータ、メタデータおよび暗号化ビデオデータを多重化し、HD-SDI フォーマットにマッピングする。マルチプレクサ／フォーマッタ 41 の出力は、パラレル／シリアル変換回路 42 でシリアルデジタルデータに変換され、スクランブラ 43 でスクランブル処理され DC 成分を除去され、NRZI 回路 44 で上述した NRZI 符号化される。NRZI 回路 44 の出力は、ケーブルドライバ 45 で伝送レベルまで増幅され、同軸ケーブル 13 に対して送り出される。

なお、HD-SDI 復号化装置 14 は、この HD-SDI 暗号化装置 12 における HD-SDI シリアル／パラレル変換回路ブロック 2

0と同様の回路（HD－SDIシリアル／パラレル変換回路ブロック20'とする）と、暗号回路ブロック30に対応する復号回路ブロックとを有する。復号回路ブロックをコンピュータで構成し、所定の記録媒体に記録された復号プログラムに従い、復号化処理を行わせても
5 よい。同軸ケーブル13を介して供給されたHD－SDIフォーマットのデジタルデータは、HD－SDIシリアル／パラレル変換回路ブロック20'において上述のHD－SDIシリアル／パラレル変換回路ブロック20と同様の処理がなされ、暗号化ビデオデータ、オーディオデータおよびメタデータが取り出される。暗号化ビデオデータ
10 は、復号回路ブロックに供給され外部のコンピュータ装置から供給された鍵（K）を用いて復号化され、ベースバンドのビデオデータが復元される。復元されたデータのうち、ビデオデータおよびメタデータは、プロジェクタ16に供給される。また、オーディオデータは、図示されないオーディオシステムに供給される。

15 第10図は、この発明の実施の一形態による暗号化回路31の一例の構成を示す。この発明の実施の一形態による暗号化回路31は、カウンタモードによるデータエラーからの復元性と、CFBモードによる、データ窃取に対する堅牢性とを兼ね備えた構成を実現している。

暗号器105は、128ビットの長さの鍵（K）を用いてAESによる暗号化を施すAES暗号器である。なお、暗号器105において利用可能な暗号化方式は、AESに限られない。DESなどのデータをブロック化して暗号化する方式であれば、他の暗号化方式を用いることもできる。また、鍵（K）のデータ長も128ビットに限定されない。

25 CPU＋タイミングコントローラ110は、第9図に示したCPU32と、図示されないタイミングコントローラからなる。タイミング

コントローラは、クロックと共に、ビデオデータのフレームおよびラインに対応したタイミングで各種信号を出力することができる。

暗号化回路 31 に対して、1 画素分のデータが輝度 Y および色差 C それぞれ 10 ビットずつを割り当てたデータ幅が 20 ビットからなる
5 ビデオデータが、クロック毎に 1 画素ずつ入力される。このビデオデータは、EXOR 回路 100 に供給され、後述する P/P シフトレジスタ 106 の出力との排他論理和をとられ、暗号化ビデオデータとされて出力される。

EXOR 回路 100 から出力された暗号化ビデオデータは、外部す
10 なわち HD-SDI パラレル/シリアル変換回路ブロック 40 に対して出力される。それと共に、暗号化ビデオデータは、フリップフロップ (FF) 回路 101 に供給され、ホールドされる。FF 回路 101 は、AES 暗号器 105 と同一のクロック 107 によりホールド値が更新される。また、FF 回路 101 は、ビデオデータのラインが更新
15 される毎に所定の回数リセットするように、CPU+タイミングコントローラ 110 からリセット信号 119 が供給される。リセット信号 119 の回数は、例えば、AES 暗号器 105 へのリセット値が AES 暗号器 105 の出力に反映される、AES レーテンシ分に対応した回数とされる。

20 なお、この実施の一形態では、FF 回路 101 に対して、データ幅が 20 ビットの暗号化ビデオデータのうち一部、例えば 16 ビットだけが入力される。用いられる 16 ビットは、元の暗号化ビデオデータの 20 ビットのデータ幅のうち LSB 側、MSB 側のうち何れでもよいし、20 ビットの中から所定の 16 ビットを用いてもよい。なお、
25 これはこの例に限らず、FF 回路 101 に対して暗号化ビデオデータの 20 ビット全てを入力することもできるし、16 ビットより少ない

ビット数で入力するようにしてもよい。

ラインカウンタ 102 は、CPU+タイミングコントローラ 110 からビデオデータのライン毎に供給されるトリガ信号 118 によりカウント値を更新するカウンタである。例えば、ラインカウンタ 102 は、ビデオデータのライン毎に、カウント値を 1 だけカウントアップする。また、ラインカウンタ 102 は、フレームが更新される毎に 1 回リセットされるように、CPU+タイミングコントローラ 110 からリセット信号 117 が供給される。ラインカウント値は、例えば 16 ビットのデータである。

10 なお、ラインカウンタ 102 は、この例に限られず、複数ライン毎にカウント値を更新するようにしてもよい。また、カウント値の更新も、1 ずつカウントするのに限られず、2 以上の所定値毎にカウントアップしてもよいし、所定値からカウントダウンするようにしてもよい。さらに、リセット信号 117 によるリセットの際にカウント値が
15 0 になるようにリセットしてもよいし、0 以外の所定値になるようにリセットすることもできる。さらにまた、ラインカウント値のデータ長は 16 ビットに限られない。

フレームカウンタ 103 は、CPU+タイミングコントローラ 110 からビデオデータのフレーム毎に供給されるトリガ信号 116 によりカウント値を更新するカウンタである。例えば、フレームカウンタ 103 は、ビデオデータのフレーム毎に、カウント値を 1 だけカウントアップする。フレームカウンタ 103 は、例えばビデオデータのプログラムの開始時に 1 回リセットするように、CPU+タイミングコントローラ 110 からリセット信号 114 が供給される。フレームカ
20 ウント値は、例えば 24 ビットのデータである。

なお、フレームカウンタ 103 は、この例に限られず、カウント値

の更新を、1 ずつカウントするのに限られず、2 以上の所定値毎にカウントアップしてもよいし、所定値からカウントダウンするようにしてもよい。また、リセット信号 1 1 7 によるリセットの際にカウント値が 0 になるようにリセットしてもよいし、0 以外の所定値になるようにリセットすることもできる。さらに、リセット信号 1 1 4 も、プログラムの先頭でリセットするのに限らず、例えば所定数のフレーム数毎にリセットするようなものでもよい。さらにまた、ラインカウン

5 値のデータ長は 1 6 ビットに限られない。

FF 回路 1 0 4 は、CPU+タイミングコントローラ 1 1 0 から与えられるデータ 1 1 2 をホールドする。このデータ 1 1 2 は、上述したフレームやラインのデータとは異なるデータであって、例えばバージョン情報といった固定値を用いてもよいし、所定の規則、例えばトリガ信号 1 1 3 に基づく所定のタイミングで更新される値であってもよい。FF 回路 1 0 4 の出力は、例えば 7 2 ビットのデータである。

10 FF 回路 1 0 4 の出力は、リセット信号 1 1 1 により所定のタイミングでリセットすることができる。なお、FF 回路 1 0 4 の出力のデータ長は、7 2 ビットに限定されない。

上述の FF 回路 1 0 4、フレームカウンタ 1 0 3、ラインカウンタ 1 0 2 および FF 回路 1 0 1 にそれぞれホールドされたデータは、AES 暗号器 1 0 5 のクロックタイミングで並列的に AES 暗号器 1 0 5 に読み出される。すなわち、この第 1 0 図の例では、FF 回路 1 0 4 にホールドされた 7 2 ビットのデータと、フレームカウンタ 1 0 3 にホールドされた 2 4 ビットのデータと、ラインカウンタ 1 0 2 にホールドされた 1 6 ビットのデータと、FF 回路 1 0 1 にホールドされた 1 6 ビットのデータとからなる 1 2 8 ビットのデータが、AES 暗号器 1 0 5 のクロックタイミングで、AES 暗号器 1 0 5 に入力され

20

25

る。

一方、CPU+タイミングコントローラ110からAES暗号器105に対して、鍵長が128ビットの鍵(K)が与えられる。AES暗号器105は、上述のFF回路104、フレームカウンタ103、
5 ラインカウンタ102およびFF回路101から入力された128ビットのデータに対して、鍵(K)を用いて暗号化を施す。暗号化されて得られた128ビットの暗号化データは、そのうちの所定の120ビットだけがP/Pシフトレジスタ106に供給される。

P/Pシフトレジスタ106は、供給された120ビットの暗号化
10 データを、入力されるビデオデータのデータ幅に合わせて20ビットずつに分割する。したがって、AES暗号器105を動作させるためのクロックは、画像データに同期したクロックの1/6の周波数となっている。P/Pシフトレジスタ106から出力された20ビットのデータがEXOR回路100に供給される。EXOR回路100では
15 、上述したように、入力されたビデオデータとP/Pシフトレジスタ106からの出力との排他論理和をとることで、入力されたビデオデータを暗号化して出力する。

このように、この発明による暗号化回路31では、暗号化された暗号化データをAES暗号器105の入力にフィードバックしているため、従来技術で第7図を用いて説明したようなデータ窃取方法で暗号化画像データを窃取して元の画像データを復元しようとしても、元の画像データを全く復元することができない。これは、CFBモードの特徴として、暗号器で発生される疑似乱数列が入力データ列に影響されるため、従来技術で説明した窃取方法により得られた疑似乱数列と
25 、暗号化回路31においてAES暗号器105で発生される疑似乱数列とが全く異なるからである。

また、暗号化データをA E S暗号器105の入力にフィードバックさせる際に、フィードバックする暗号化データをホールドするF F回路104に対してライン毎のリセットを行っているため、前ラインでの暗号化データによるフィードバックの影響が全くなくなる。したがって、前ラインで同期外れや画素欠落などの事故が生じた場合、C F Bモードでは当該ライン上にある暗号データの復号は不可能であるが、本発明の方式によれば、ラインが更新された際に完全に復帰できることを意味する。

なお、上述では、A E S暗号器105に入力されるデータをF F回路104、フレームカウンタ103、ラインカウンタ102およびF F回路101の出力としたが、これはこの例に限定されない。例えば、F F回路104による固定値出力を省略することができる。また、フレームカウンタ103およびラインカウンタ102に対して更新およびリセット周期が異なるカウンタをさらに追加してもよいし、フレームカウンタ103を省略することも可能である。さらに、上述では、F F回路104、フレームカウンタ103、ラインカウンタ102およびF F回路101の出力データのビット配分を、F F回路104が72ビット、フレームカウンタ103が24ビット、ラインカウンタ102およびF F回路101がそれぞれ16ビットとしたが、これはこの例に限定されず、他のビット配分でもよい。さらにまた、入力されるビデオデータのビット幅も、20ビットに限定されず、ビデオ信号の形式も輝度Y、色差Cによるものに限定されない。

ここで、特許請求の範囲との一例の対応関係を示すと、請求項1において、保持手段は、例えばF F回路101に対応する。1または複数のカウンタは、例えばフレームカウンタ103およびラインカウンタ102に対応する。暗号化手段は、例えばA E S暗号器105に対

応する。演算手段は、例えばE X O R回路1 0 0に対応する。演算手段から出力された暗号化データの一部または全部を保持手段に入力する経路は、例えばE X O R回路1 0 0の出力がF F回路1 0 1に供給される経路に対応する。信号発生手段は、例えばC P U + タイミング
5 コントローラ1 1 0に対応する。なお、これらの対応関係は一例であって、これに限定されるものではない。

第1 1 図は、第1 0 図に示す暗号化回路3 1に対応する復号化回路1 5 0の一例の構成を示す。この復号化回路1 5 0は、H D - S D I 復号装置1 4に組み込まれて用いられ、H D - S D I 暗号化装置1 2
10 から同軸ケーブル1 3を介して伝送された暗号化ビデオデータを復号化する。復号化回路1 5 0は、暗号化回路3 1におけるF F回路1 0 1に対して入力される暗号化ビデオデータの入力経路が異なる以外、同一の構成で実現できる。また、復号化回路1 5 0において、各種のタイミングやデータのビット幅などは、上述の暗号化回路3 1と対応
15 させられる。

復号化回路1 5 0において、A E S暗号器1 2 5は、上述した暗号化回路3 1で用いられるA E S暗号器1 0 5と同一の回路であって、入力されたデータに対して、暗号化回路3 1と共通の鍵である1 2 8 ビットの長さの鍵（K）を用いてA E Sによる暗号化を施す。また、
20 C P U + タイミングコントローラ1 3 0は、C P Uとタイミングコントローラからなる。タイミングコントローラは、クロックと共に、ビデオデータのフレームおよびラインに対応したタイミングで各種信号を出力することができる。

復号化回路1 5 0に対して、1画素分に対応する暗号化ビデオデータがデータ幅2 0 ビットで以てクロック毎に入力される。この暗号化
25 ビデオデータは、E X O R回路1 2 0に供給され、後述するP / Pシ

フトレジスタ 1 2 6 の出力との排他論理和をとられ、暗号化ビデオデータが復号化され元のデータが復元された復元ビデオデータとされて出力される。

暗号化ビデオデータは、E X O R 回路 1 2 0 に供給されると共に、
5 2 0 ビットのうち上述の F F 回路 1 0 1 で用いられたのに対応する 1 6 ビットが F F 回路 1 2 1 に供給され、ホールドされる。勿論、上述の F F 回路 1 0 1 において入力ビデオデータの 2 0 ビットの全てが用いられた場合、F F 回路 1 2 1 には、暗号化ビデオデータの 2 0 ビット全てが入力される。F F 回路 1 2 1 は、A E S 暗号器 1 2 5 と同一
10 のクロック 1 4 0 によりホールド値が更新される。また、F F 回路 1 2 1 は、ビデオデータのラインが更新される毎に所定の回数リセットするように、C P U + タイミングコントローラ 1 3 0 からリセット信号 1 3 9 が供給される。リセット信号 1 3 9 のタイミングは、例えば、A E S 暗号器 1 2 5 へのリセット値が A E S 暗号器 1 2 5 の出力に
15 反映される、A E S レーテンシ分とされる。

ラインカウンタ 1 2 2 は、上述のラインカウンタ 1 0 2 に対応して更新されるカウンタであり、C P U + タイミングコントローラ 1 3 0 から暗号化ビデオデータのライン毎に供給されるトリガ信号 1 3 8 により、例えば暗号化ビデオデータのライン毎にカウント値を 1 だけカ
20 ウントアップしてカウント値を更新する。また、ラインカウンタ 1 2 2 は、フレームが更新される毎に 1 回リセットされるように、C P U + タイミングコントローラ 1 3 0 からリセット信号 1 3 7 が供給される。ラインカウント値は、例えば 1 6 ビットのデータである。

フレームカウンタ 1 2 3 は、上述のフレームカウンタ 1 0 3 に対応
25 して更新されるカウンタであり、C P U + タイミングコントローラ 1 3 0 から暗号化ビデオデータのフレーム毎に供給されるトリガ信号 1

36により、例えば暗号化ビデオデータのフレーム毎にカウント値を1だけカウントアップしてカウント値を更新するカウンタである。フレームカウンタ123は、例えば暗号化ビデオデータのプログラムの開始時に1回リセットするように、CPU+タイミングコントローラ130からリセット信号134が供給される。フレームカウント値は、例えば24ビットのデータである。

FF回路124は、CPU+タイミングコントローラ130から与えられるデータ132をホールドする。このデータ132は、上述したフレームやラインのデータとは異なるデータであって、例えばバージョン情報といった固定値を用いてもよいし、所定の規則、例えばトリガ信号133に基づく所定のタイミングで更新される値であってもよい。例えば、このデータ132は、上述のデータ112に対応する値が用いられる。上述したように、データ112としてトリガ信号113に基づく所定のタイミングで更新される値を用いたときは、データ132は、例えば、トリガ113に対応するトリガ信号133に基づく所定のタイミングで更新される値ととすることができる。FF回路124の出力は、例えば72ビットのデータである。FF回路124の出力は、上述のリセット信号111に対応するタイミングのリセット信号131によりリセットすることができる。

20 上述のFF回路124、フレームカウンタ123、ラインカウンタ122およびFF回路121にそれぞれホールドされたデータは、AES暗号器125のクロックタイミングで並列的にAES暗号器125に読み出される。すなわち、この第11図の例では、FF回路124にホールドされた72ビットのデータと、フレームカウンタ123にホールドされた24ビットのデータと、ラインカウンタ122にホールドされた16ビットのデータと、FF回路121にホールドされ

た16ビットのデータとからなる128ビットのデータが、AES暗号器125のクロックタイミングで、AES暗号器125に入力される。

一方、CPU+タイミングコントローラ130からAES暗号器125に対して、鍵長が128ビットの鍵(K)が与えられる。この鍵(K)は、上述した暗号化回路31で用いられる鍵(K)と共通する鍵である。AES暗号器125は、上述のFF回路124、フレームカウンタ123、ラインカウンタ122およびFF回路121から入力された128ビットのデータに対して、鍵(K)を用いて暗号化を
10 施す。暗号化されて得られた128ビットの暗号化データは、そのうちの所定の120ビットだけがP/Pシフトレジスタ126に供給される。

P/Pシフトレジスタ126は、供給された120ビットの暗号化データを、入力される暗号化ビデオデータのデータ幅に合わせて20
15 ビットずつに分割する。したがって、AES暗号器125を動作させるためのクロックは、画像データに同期したクロックの1/6の周波数となっている。P/Pシフトレジスタ126から出力された20ビットのデータがEXOR回路120に供給される。EXOR回路120では、上述したように、入力された暗号化ビデオデータとP/Pシフトレジスタ126からの出力との排他論理和をとることで、入力さ
20 れた暗号化ビデオデータを復号化して出力する。

上述したように、この復号化回路150は、上述の暗号化回路31に対応するものである。したがって、AES暗号器125にデータを入力するFF回路124、フレームカウンタ123、ラインカウンタ
25 122およびFF回路121の構成や動作は、上述の暗号化回路31におけるFF回路104、フレームカウンタ103、ラインカウンタ

1 0 2 および F F 回路 1 0 1 に対応する。

ここで、特許請求の範囲との一例の対応関係を示すと、請求項 1 0
において、保持手段は、例えば F F 回路 1 2 1 に対応する。1 または
複数のカウンタは、例えばフレームカウンタ 1 2 3 およびラインカウ
5 ンタ 1 2 2 に対応する。暗号化手段は、例えば A E S 暗号器 1 2 5 に
対応する。演算手段は、例えば E X O R 回路 1 2 0 に対応する。外部
から入力された暗号化データの一部または全部を保持手段に入力する
経路は、例えば暗号化ビデオデータが E X O R 回路 1 2 0 に入力され
ると共に F F 回路 1 2 1 に供給される経路に対応する。信号発生手段
10 は、例えば C P U + タイミングコントローラ 1 3 0 に対応する。なお
、これらの対応関係は一例であって、これに限定されるものではない
。

なお、ここでは、入力されたビデオデータに対して P / P シフトレ
ジスタ 1 0 6 の出力を作用させ、暗号化ビデオデータを得るために E
15 X O R 回路 1 0 0 を用いているが、これはこの例に限定されない。

また、上述では、ビデオデータ、暗号化ビデオデータの伝送を H D
- S D I の規格に基づき行うように説明したが、これはこの例に限定
されるものではなく、この発明は、他の伝送方式に対しても適用可能
である。

請 求 の 範 囲

1. 入力されたデータの一部または全部をトリガ信号により保持し、上記保持された上記データをリセット信号によりリセットする保持手段と、

- 5 トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする1または複数のカウンタと、

 上記保持手段で保持された上記データと上記1または複数のカウンタによる1または複数の上記カウント値とを暗号化する暗号化手段と

10 、

 上記暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算手段と、

- 上記演算手段から出力された上記暗号化データの一部または全部を
15 上記保持手段に入力する経路と、

 上記保持手段および上記1または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持手段および上記1または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段と

- 20 を有することを特徴とする暗号装置。

2. 請求の範囲1に記載の暗号装置において、

 上記暗号化手段に対して、さらに固定値が入力され、上記暗号化手段は、該固定値と上記保持手段で保持された上記データと上記1または複数のカウント値とを暗号化するようにしたことを特徴とする暗号

- 25 装置。

3. 請求の範囲1に記載の暗号装置において、

上記保持手段に上記保持された上記データをリセットするリセット信号は、上記 1 また複数のカウンタのうち少なくとも 1 の上記カウンタに与えられるリセット信号と同期したタイミングで上記保持手段に与えられることを特徴とする暗号装置。

- 5 4. 請求の範囲 1 に記載の暗号装置において、

上記入力データは映像データであって、上記保持手段をリセットするリセット信号は上記映像データに同期していることを特徴とする暗号装置。

5. 請求の範囲 4 に記載の暗号装置において、

- 10 上記保持手段をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする暗号装置。

6. 請求の範囲 1 に記載の暗号装置において、

- 15 上記入力データは映像データであって、上記 1 または複数のカウンタのうち少なくとも 1 をリセットするリセット信号は上記映像データに同期していることを特徴とする暗号装置。

7. 請求の範囲 6 に記載の暗号装置において、

上記 1 または複数のカウンタのうち少なくとも 1 をリセットするリセット信号は上記映像データのフレームに同期していることを特徴とする暗号装置。

- 20 8. 請求の範囲 6 に記載の暗号装置において、

上記 1 または複数のカウンタのうち少なくとも 1 をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする暗号装置。

9. 入力されたデータの一部または全部をトリガ信号により保持し、
25 上記保持された上記データをリセット信号によりリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする
1 または複数のカウントのステップと、

- 上記保持のステップで保持された上記データと上記 1 または複数の
5 カウントのステップによる 1 または複数の上記カウント値とを暗号化する暗号化のステップと、

上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

- 10 上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

上記保持のステップおよび上記 1 または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記 1 または複数のカウンタのそれぞれに所定の規則および／またはタ

- 15 イミングで発生する信号発生 of ステップと
を有することを特徴とする暗号方法。

1 0. 入力されたデータの一部または全部をトリガ信号により保持し、上記保持された上記データをリセット信号によりリセットする保持のステップと、

- 20 トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする
1 または複数のカウントのステップと、

上記保持のステップで保持された上記データと上記 1 または複数のカウントのステップによる 1 または複数の上記カウント値とを暗号化
25 する暗号化のステップと、

上記暗号化のステップの出力と外部から入力された入力データとを

用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

- 5 上記保持のステップおよび上記 1 また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記 1 また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップと

を有する暗号方法をコンピュータ装置に実行させることを特徴とする

10 暗号プログラム。

1 1. 入力されたデータの一部または全部をトリガ信号により保持し、上記保持された上記データをリセット信号によりリセットする保持のステップと、

- 15 トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする 1 または複数のカウンタのステップと、

上記保持のステップで保持された上記データと上記 1 または複数のカウンタのステップによる 1 または複数の上記カウント値とを暗号化する暗号化のステップと、

- 20 上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

- 25 上記保持のステップおよび上記 1 また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび

上記 1 また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生ステップと

を有する暗号方法をコンピュータ装置に実行させる暗号プログラムが記録されたことを特徴とするコンピュータ装置に読み取り可能な記録

5 媒体。

- 1 2. 入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする 1 または複数のカウンタと、上記保持手段で保持された上記データと上記 1 または複数のカウンタによる 1 または複数の上記カウント値とを暗号化する暗号化手段と、上記暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算手段と、上記演算手段から出力された上記暗号化データの一部または全部を上記保持手段に入力する経路と、上記保持手段および上記 1 または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持手段および上記 1 または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有する暗号装置で暗号化された上記暗号化データを復号する復号装置において、
- 10
15
20

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持手段と、

- 25 トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする

1 または複数のカウンタと、

上記保持手段で保持された上記データと上記 1 または複数のカウンタによる 1 または複数の上記カウント値とを暗号化する暗号化手段と

、

- 5 上記暗号化手段の出力と外部から入力された暗号化データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算手段と、

上記外部から入力された上記暗号化データの一部または全部を上記保持手段に入力する経路と、

- 10 上記保持手段および上記 1 または複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持手段および上記 1 または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段と

を有することを特徴とする復号装置。

- 15 1 3. 請求の範囲 1 2 に記載の復号装置において、

上記暗号化手段に対して、さらに固定値が入力され、上記暗号化手段は、該固定値と上記保持手段で保持された上記データと上記 1 または複数のカウント値とを暗号化するようにしたことを特徴とする復号装置。

- 20 1 4. 請求の範囲 1 2 に記載の復号装置において、

上記保持手段に上記保持された上記データをリセットするリセット信号は、上記 1 または複数のカウンタのうち少なくとも 1 の上記カウンタに与えられるリセット信号と同期したタイミングで上記保持手段に与えられることを特徴とする復号装置。

- 25 1 5. 請求の範囲 1 2 に記載の復号装置において、

上記暗号化データは映像データが暗号化されたデータであって、上

記保持手段をリセットするリセット信号は上記映像データに同期していることを特徴とする復号装置。

16. 請求の範囲15に記載の復号装置において、

上記保持手段をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする復号装置。

17. 請求の範囲12に記載の復号装置において、

上記暗号化データは映像データが暗号化されたデータであって、上記1または複数のカウンタのうち少なくとも1をリセットするリセット信号は上記映像データに同期していることを特徴とする復号装置。

10 18. 請求の範囲17に記載の復号装置において、

上記1または複数のカウンタのうち少なくとも1をリセットするリセット信号は上記映像データのフレームに同期していることを特徴とする復号装置。

19. 請求の範囲17に記載の復号装置において、

15 上記1または複数のカウンタのうち少なくとも1をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする復号装置。

20. 入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持
20 のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする1または複数のカウンタのステップと、上記保持のステップで保持された上記データと上記1または複数のカウンタのステップによる1または複数の上記カウント値とを暗号化する暗号化のステップと、上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入
25

カデータが該暗号化された暗号化データを出力する演算のステップと、
上記演算のステップから出力された上記暗号化データの一部または
全部を上記保持のステップに入力するステップと、上記保持のステッ
5 5 5
プおよび上記 1 また複数のカウンタのそれぞれに与えるトリガ信号お
よびリセット信号を、上記保持のステップおよび上記 1 また複数のカ
ウンタのそれぞれに所定の規則および／またはタイミングで発生する
信号発生 of the ステップとを有する暗号方法で暗号化された上記暗号化デ
ータを復号する復号方法において、

10 入力されたデータの一部または全部をトリガ信号により保持し、リ
セット信号により上記保持された上記データをリセットする保持のス
テップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウ
ンし、リセット信号により上記カウント値を所定の値にリセットする
1 または複数のカウンタのステップと、

15 上記保持のステップで保持された上記データと上記 1 または複数の
カウンタのステップによる 1 または複数の上記カウント値とを暗号化
する暗号化手段と、

上記暗号化のステップの出力と外部から入力された暗号化データと
を用いて所定の規則で演算して上記入力データを暗号化し、該入力デ
20 ータが該暗号化された暗号化データを出力する演算のステップと、

上記外部から入力された上記暗号化データの一部または全部を上記
保持のステップに入力するステップと、

上記保持のステップおよび上記 1 また複数のカウンタのそれぞれに
与えるトリガ信号およびリセット信号を、上記保持のステップおよび
25 上記 1 また複数のカウンタのそれぞれに所定の規則および／またはタ
イミングで発生する信号発生 of the ステップと

を有することを特徴とする復号方法。

2 1. 入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたは
5 カウントダウンし、リセット信号により上記カウント値を所定の値にリセットする 1 または複数のカウントのステップと、上記保持のステップで保持された上記データと上記 1 または複数のカウントのステップによる 1 または複数の上記カウント値とを暗号化する暗号化のステップと、上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、上記保持のステップおよび上記 1 または複数のカウントのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記 1 または複数のカウントのそれぞれに所定の規則および／またはタイミングで発生する信号発生
15 のステップとを有する暗号方法で暗号化された上記暗号化データを復号する復号方法をコンピュータ装置に実行させる復号プログラムにおいて、

20 上記復号方法は、

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする
25 1 または複数のカウントのステップと、

上記保持のステップで保持された上記データと上記 1 または複数のカウンタのステップによる 1 または複数の上記カウンタ値とを暗号化する暗号化手段と、

- 上記暗号化のステップの出力と外部から入力された暗号化データと
5 を用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記外部から入力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

- 上記保持のステップおよび上記 1 または複数のカウンタのそれぞれに
10 与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記 1 または複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生
のステップと
を有することを特徴とする復号プログラム。

- 2 2. 入力されたデータの一部または全部をトリガ信号により保持し
15 、リセット信号により上記保持された上記データをリセットする保持のステップと、トリガ信号によりカウンタ値をカウンタアップまたはカウンタダウンし、リセット信号により上記カウンタ値を所定の値にリセットする 1 または複数のカウンタのステップと、上記保持のステップで保持された上記データと上記 1 または複数のカウンタのステップによる 1 または複数の上記カウンタ値とを暗号化する暗号化のステップと、上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、上記演算のステップから出力された上記暗号化データの一部または
20 全部を上記保持のステップに入力するステップと、上記保持のステップおよび上記 1 または複数のカウンタのそれぞれに与えるトリガ信号お

よびリセット信号を、上記保持のステップおよび上記 1 また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生 of the ステップとを有する暗号方法で暗号化された上記暗号化データを復号する復号方法をコンピュータ装置に実行させる復号プログラムが記録されたコンピュータ装置に読み取り可能な記録媒体において、

上記復号方法は、

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする 1 または複数のカウンタのステップと、

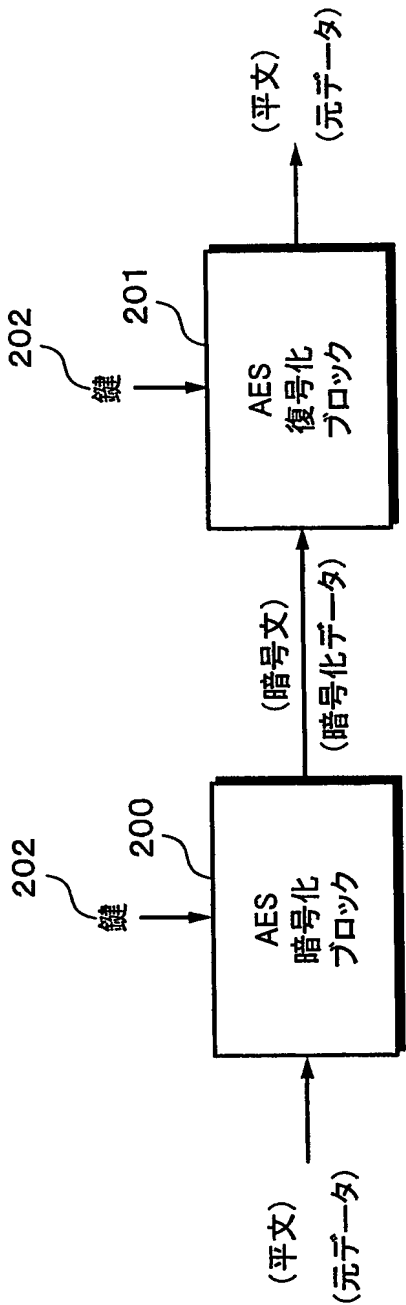
上記保持のステップで保持された上記データと上記 1 または複数のカウンタのステップによる 1 または複数の上記カウント値とを暗号化する暗号化手段と、

上記暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

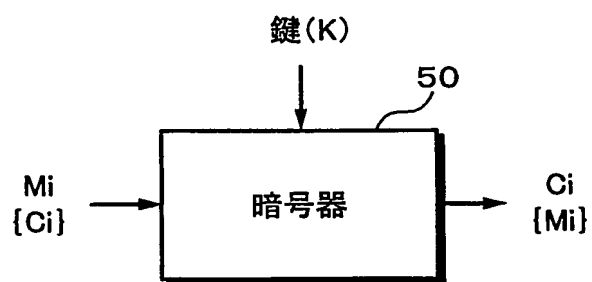
上記外部から入力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

上記保持のステップおよび上記 1 また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記 1 また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生 of the ステップとを有することを特徴とする記録媒体。

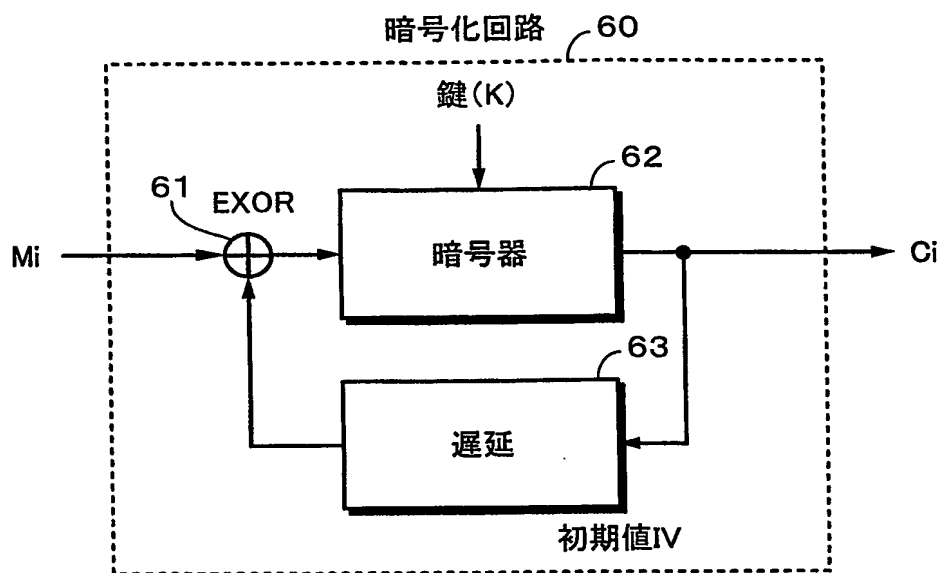
第1図



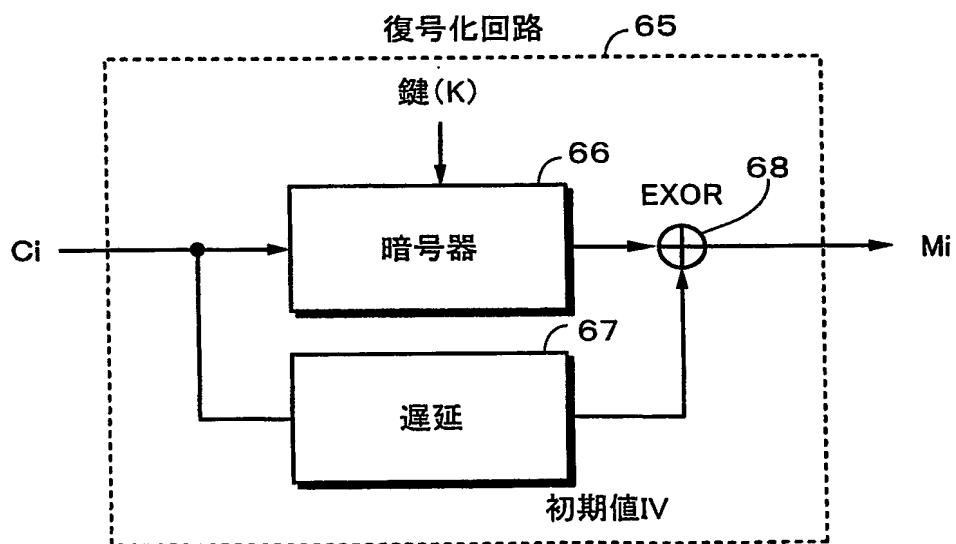
第2図



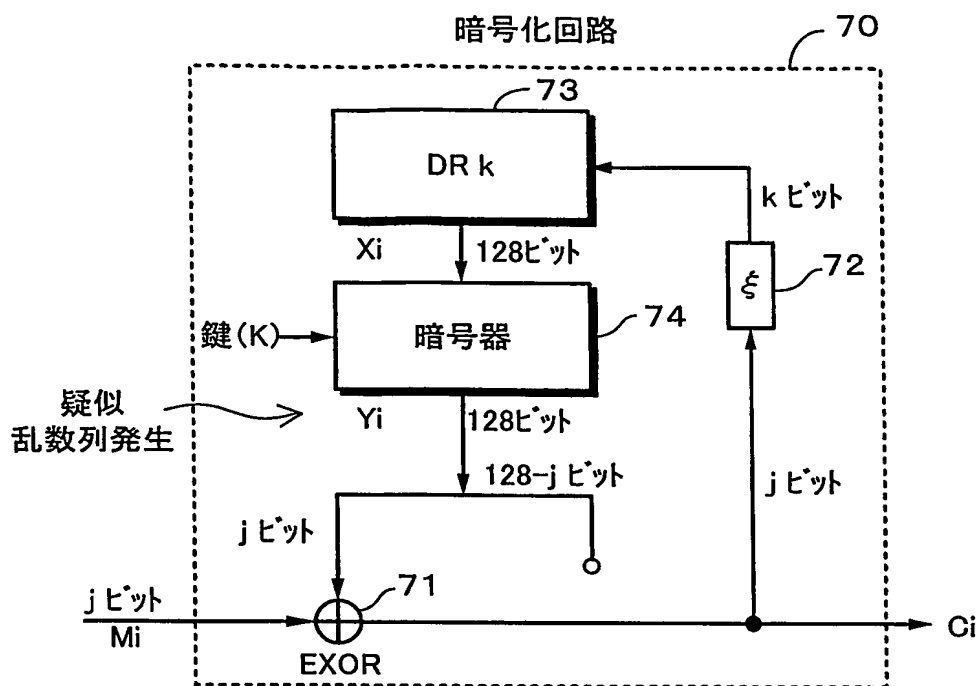
第3図A



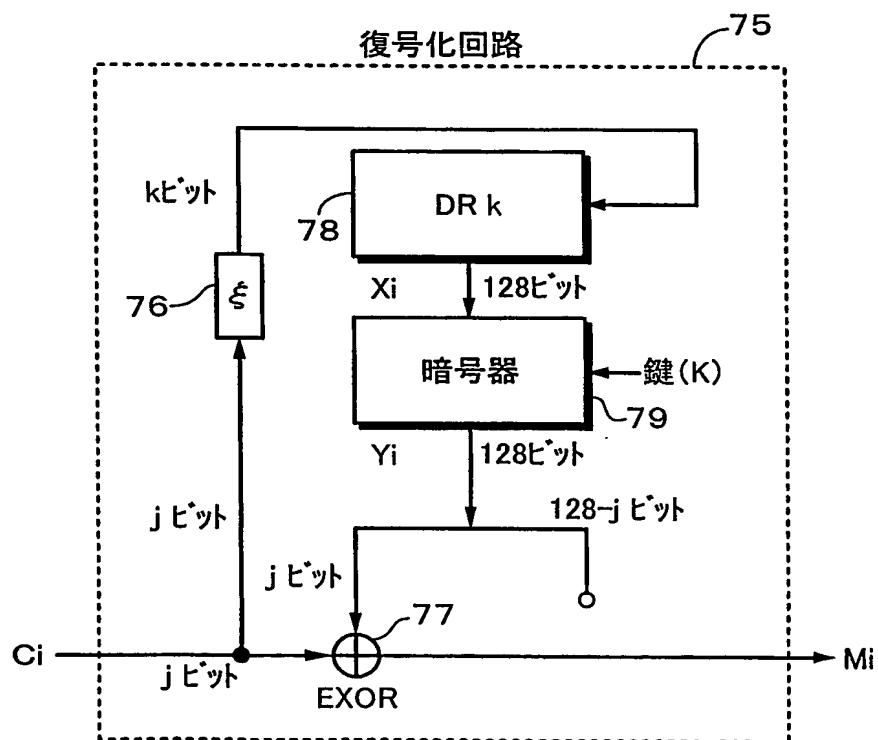
第3図B



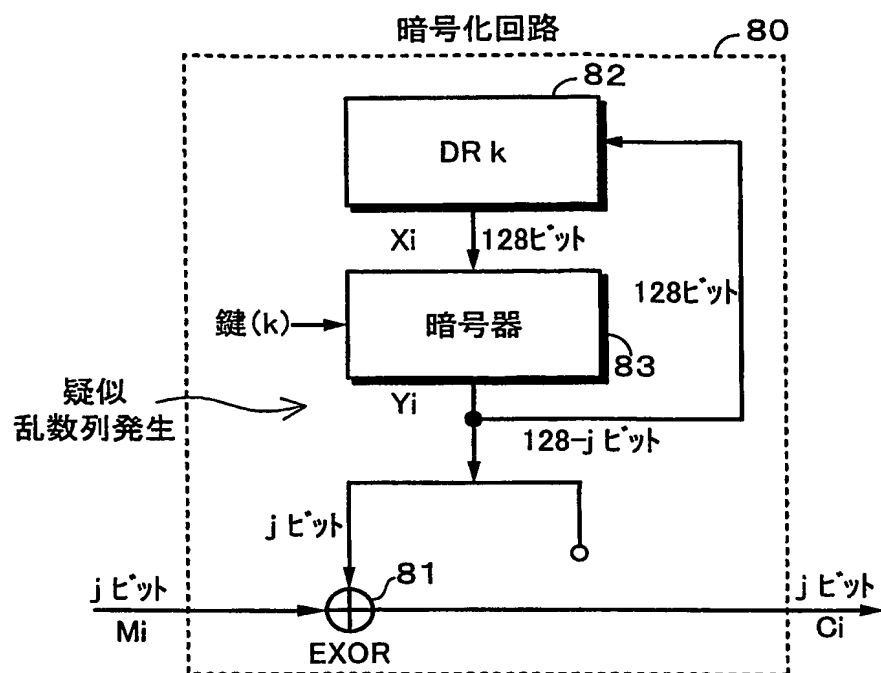
第4図A



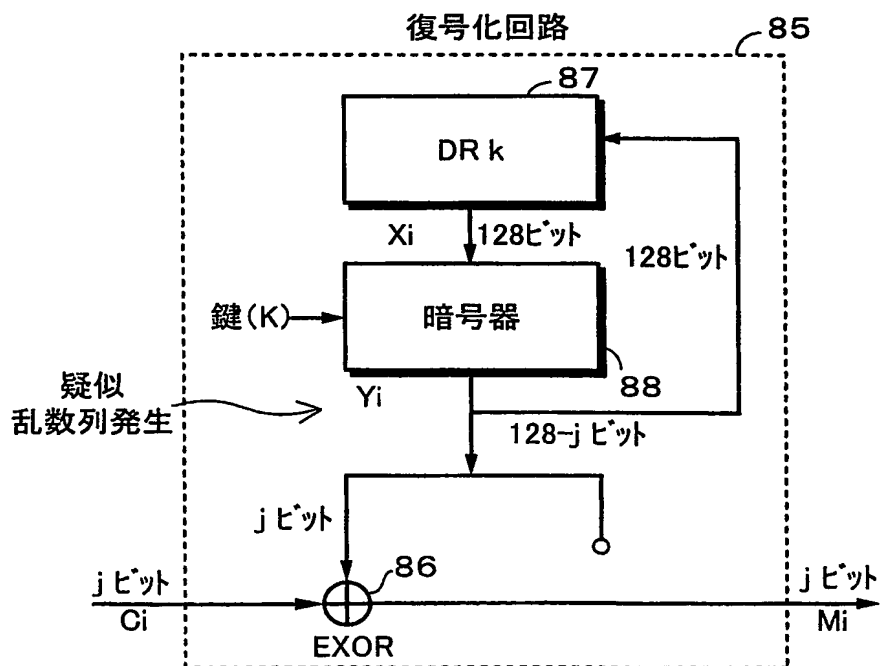
第4図B



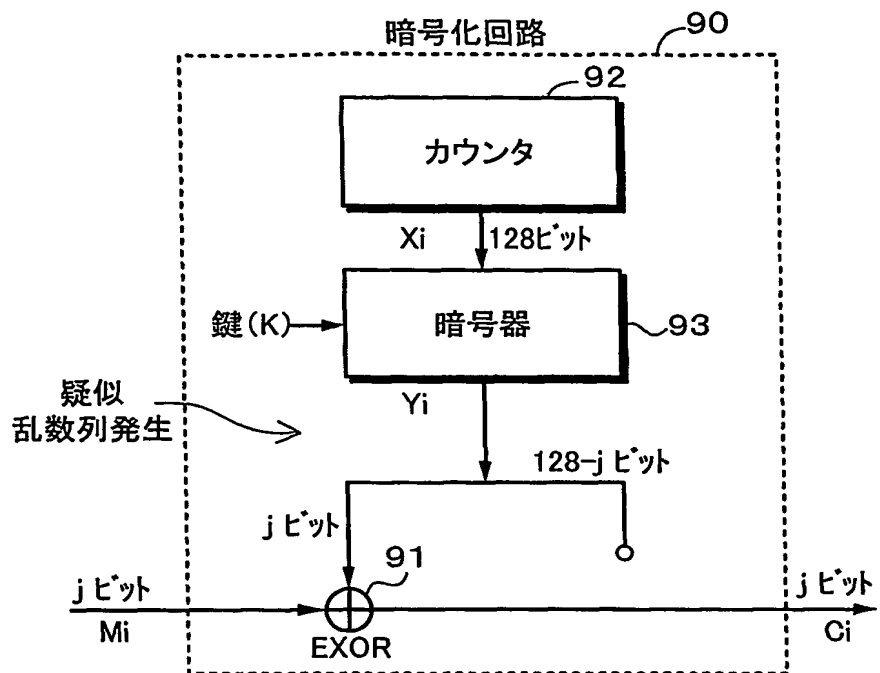
第5図A



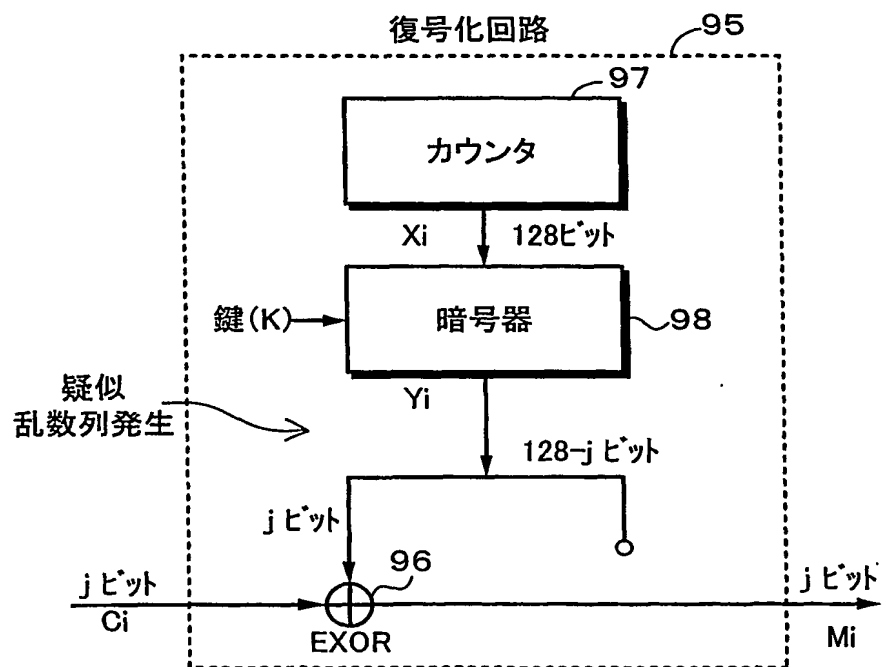
第5図B



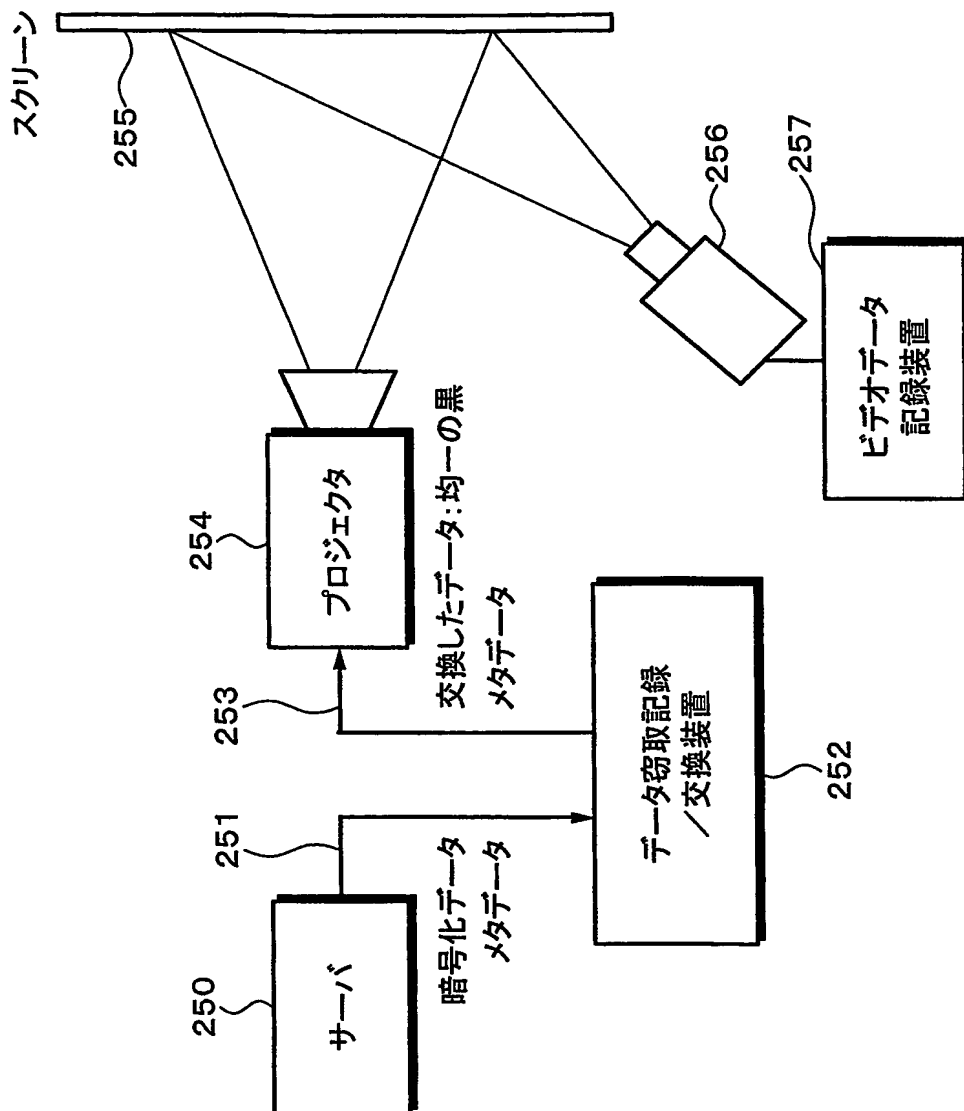
第6図A



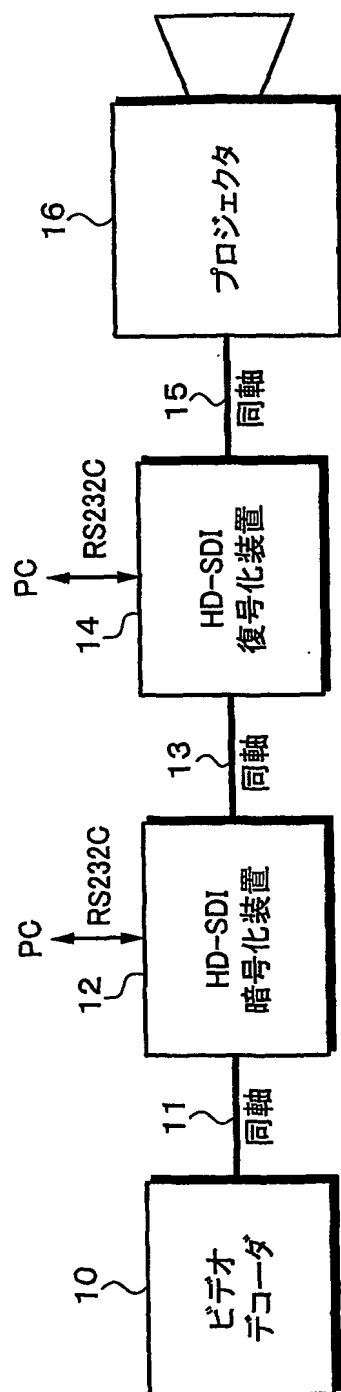
第6図B



第7図

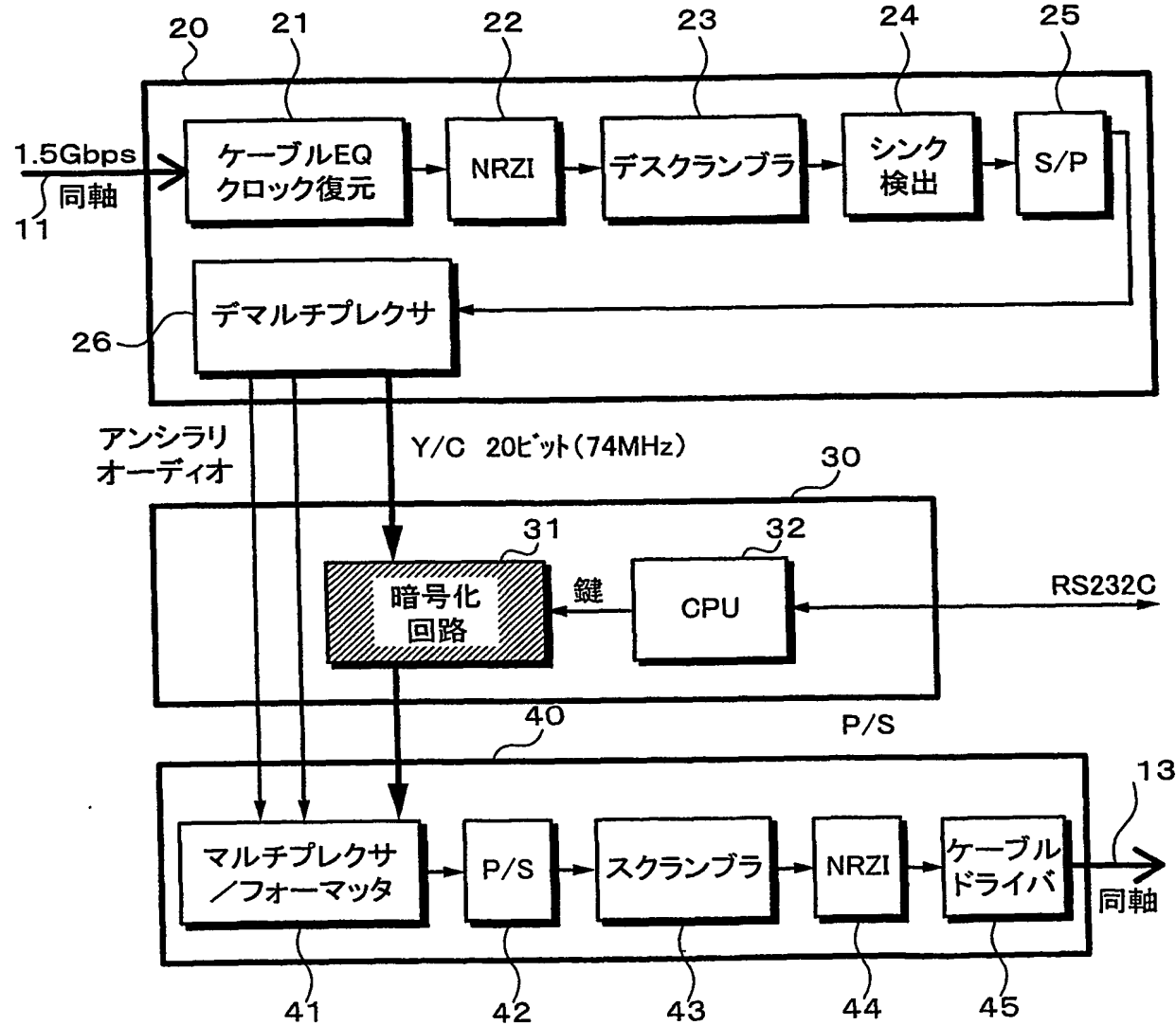


第8図



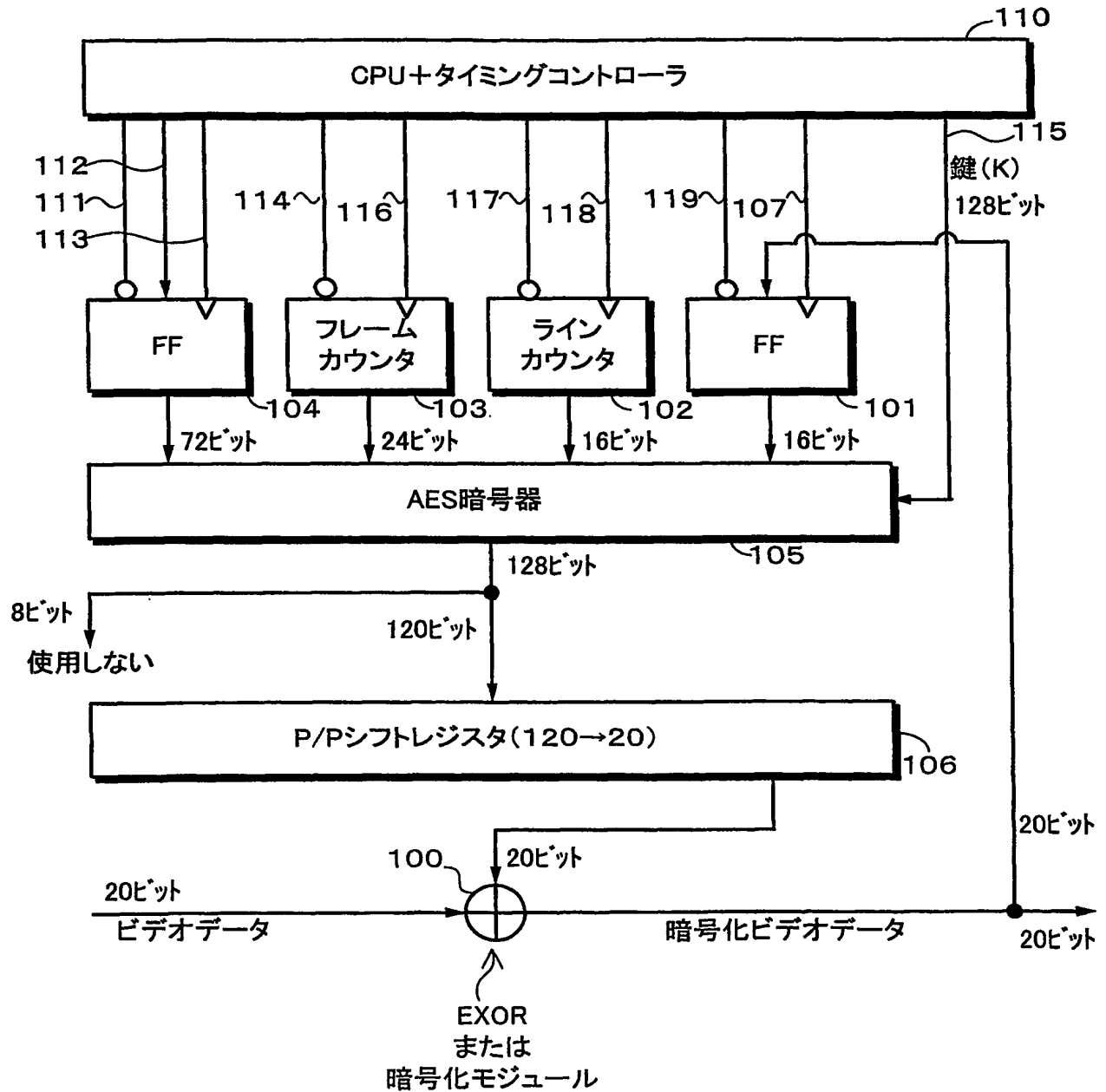
第 9 図

12

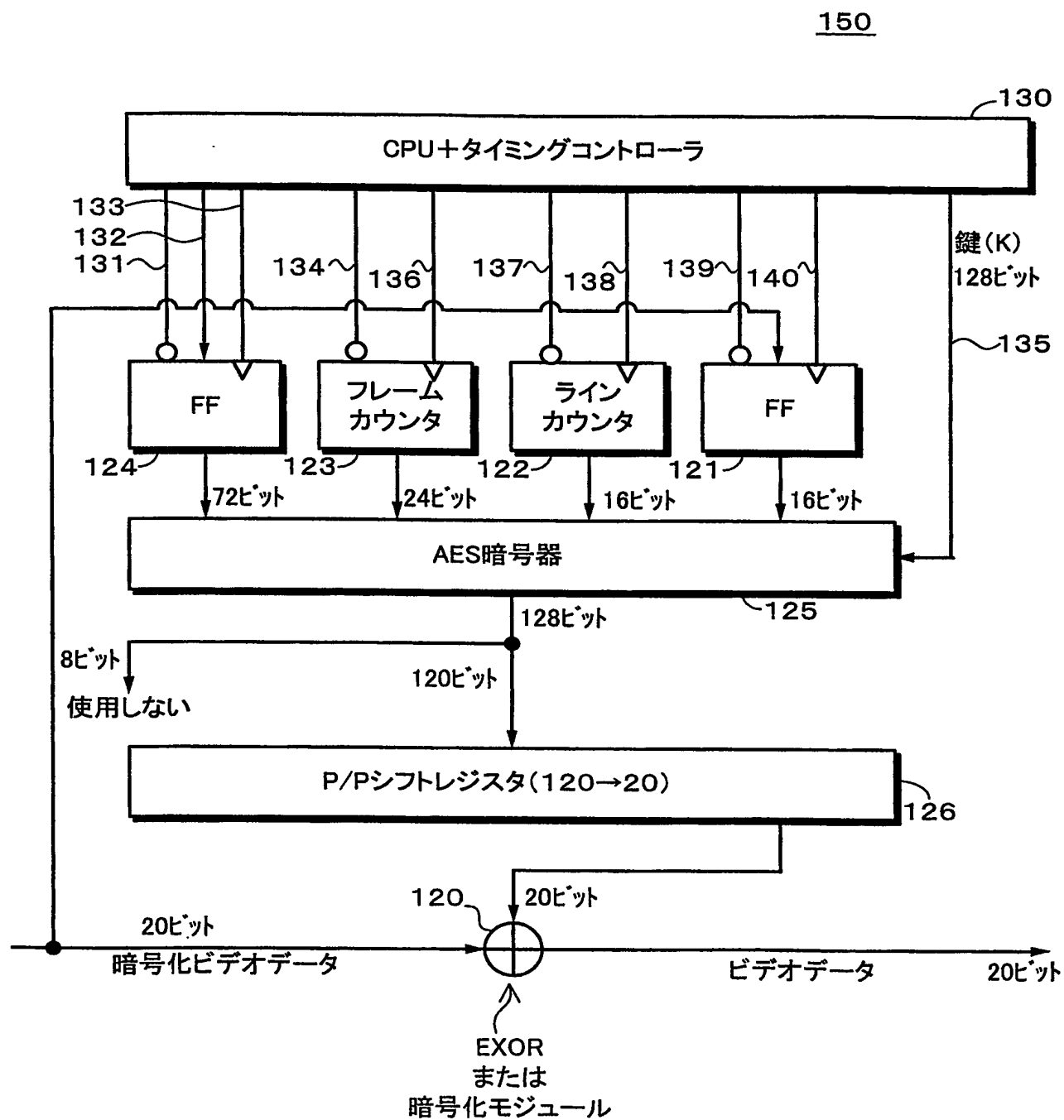


第10図

31



第 1 1 図



符 号 の 説 明

- 1 0 ビデオデコーダ
- 1 2 HD-SDI 暗号化装置
- 1 3 同軸ケーブル
- 1 4 HD-SDI 復号装置
- 1 6 プロジェクタ
- 2 0 HD-SDI シリアル／パラレル変換回路ブロック
- 2 6 デマルチプレクサ
- 3 0 暗号回路ブロック
- 3 1 暗号化回路
- 3 2 CPU
- 4 0 HD-SDI パラレル／シリアル変換回路ブロック
- 4 1 マルチプレクサ／フォーマッタ
- 5 0 復号化回路
- 1 0 0 EXOR 回路
- 1 0 1 FF 回路
- 1 0 2 ラインカウンタ
- 1 0 3 フレームカウンタ
- 1 0 4 FF 回路
- 1 0 5 AES 暗号器
- 1 0 6 P/P シフトレジスタ
- 1 1 0 CPU+タイミングコントローラ

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/009907

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G09C1/00, H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G09C1/00, H04L9/06, H04N7/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Kokai Jitsuyo Shinan Koho 1971-2004
Toroku Jitsuyo Shinan Koho 1994-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE (JOIS), block cipher, counter, feedback

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Jaechul Sung et al., Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation, Lecture Notes in Computer Science, Vol.2288, pages 103 to 113, 2002 especially 3 The CTR-OFB and CTR-CFB Schemes, Appendix: The Figures of the CTR-OFB and CTR-CFB Schemes	1-22

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
12 November, 2004 (12.11.04)

Date of mailing of the international search report
30 November, 2004 (30.11.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl⁷ G09C1/00, H04L9/06

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl⁷ G09C1/00, H04L9/06, H04N7/16

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国登録実用新案公報	1994-2004年
日本国公開実用新案公報	1971-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)
block cipher, counter, feedback

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	Jaechul Sung, et.al., Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation, Lecture Notes in Computer Science, Vol.2288, p.103-113, 2002 especially 3 The CTR-OFB and CTR-CFB Schemes, Appendix: The Figures of the CTR-OFB and CTR-CFB Schemes	1-22

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

12.11.2004

国際調査報告の発送日

30.11.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5M

9364

電話番号 03-3581-1101 内線 3599

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☒ GRAY SCALE DOCUMENTS

☒ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.